Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of claims:

1. (currently amended) A method of adding elements of a finite field ~~F_{2^m}, where m is less than a predetermined number n, said method~~ comprising the steps of:

a) storing a first element and a second element in respective ones of a pair of registers, each of said pair of registers comprising [[said]] a first predetermined number of machine words;

b) establishing an accumulator having [[said]] a second predetermined number of machine words; [[and]]

c) ~~computing~~ performing a non-reducing computation ~~for each of said machine words in said accumulator the exclusive-or~~ of the corresponding machine words representing each of said first and second elements by taking the exclusive-or of said first and second elements to obtain, in said accumulator, a representation of a unreduced result of the addition of said elements, and, upon computing said unreduced result; ~~completion of said computation~~

d) performing a specific modular reduction of said unreduced result to reduce said unreduced result to that of a field element of said finite field ~~a predetermined number of words~~.

2. (canceled)

3. (currently amended) A finite field multiplier operable to multiply two elements of a selected one of a plurality of finite fields, said finite fields being partitioned into subsets, said multiplier comprising:

a) a plurality of wordsized finite field multipliers, each suitable for multiplying elements of each finite field in a respective subset of said plurality of finite fields;

b) a finite field reducer configured to perform reduction in said selected one of said plurality of finite fields; and

c) a processor configured to:

i) operate [[the]] a corresponding one of said plurality of wordsized finite field multipliers being suitable for use with said selected one of said finite fields to perform a non-reducing computation of said two elements to obtain an

unreduced intermediate product; and

ii) upon computing said unreduced intermediate product, determine a specific modular reduction corresponding to said selected one of said finite fields and operate said finite field reducer on said unreduced intermediate product to reduce said unreduced intermediate product to that of a field element of said selected one of said finite fields to obtain the product of the two elements.

4. (currently amended) A method of performing a finite field operation on elements ~~at least one element r,~~ of a finite field, comprising the steps of:

a) representing each element as a predetermined number of machine words;

b) performing a non-reducing wordsized operation on said representations, said wordsized operation corresponding to said finite field operation;

c) completing said non-reducing wordsized operation for each word of said representations to obtain an unreduced result; and

d) upon computing said unreduced result, performing a specific modular reduction of said unreduced result to reduce said unreduced result to that of a field element of said finite field ~~a predetermined number of words~~.

5. (currently amended) A finite field engine for performing a finite field operation on elements ~~at least one element~~ of a selected finite field chosen from a set of finite fields, said set of finite fields being divided into subsets according to their word size, comprising:

a) a finite field operator for each of said subsets;

b) a finite field reducer for each of said finite fields;

c) a processor configured to choose the finite field operator corresponding to the subset containing said selected ~~chosen~~ finite field and the finite field reducer for said selected ~~chosen~~ finite field and perform a non-reducing computation by applying a plurality of applications of the chosen finite field operator to said elements to produce an unreduced intermediate result and, upon computing said unreduced intermediate result, apply the chosen finite field reducer to said unreduced intermediate result to reduce said unreduced result to that of a field element of said selected finite field to obtain the result of said finite field operation.

6. (currently amended) A cryptographic system comprising:

a) a plurality of elliptic curves, each specifying elliptic curve parameters and a respective

finite field;

b) a plurality of finite field settings corresponding to each finite field;

c) a plurality of wordsized finite fields, each having routines, each finite field being assigned to one of said wordsized finite fields;

d) a reduction routine for each finite field;

e) a computational apparatus configured to perform a cryptographic operation by the steps of:

i) selecting one of said elliptic curves; and

ii) performing a non-reducing cryptographic function using the routines from the wordsized finite field to which the respective finite field corresponding to said selected elliptic curve is assigned to obtain an unreduced result; said routines including at least one finite field operation and, upon obtaining said unreduced result ~~subsequent thereto~~, performing a modular reduction according to said respective finite field to reduce said unreduced result to that of a field element of said respective finite field to obtain a reduced result of said operation in ~~corresponding to~~ a predetermined number of words.

7. (previously presented) A method according to claim 4 wherein said modular reduction is determined by said finite field.

8. (previously presented) A method according to claim 4 wherein said finite field operation is addition.

9. (previously presented) A method according to claim 4 wherein said finite field operation is subtraction.

10. (previously presented) A method according to claim 4 wherein said finite field operation is multiplication.